On the Design of Secure Block Ciphers

Howard M. Heys and Stafford E. Tavares

Department of Electrical and Computer Engineering
Queen's University
Kingston, Ontario K7L 3N6
email: tavares@ee.queensu.ca

Abstract — In this paper, we examine a class of block ciphers referred to as substitution-permutation networks or SPNs. We assert that the basic SPN architecture can be used to provide an efficient implementation of a secure block cipher if the system S-boxes are carefully selected and connected with an appropriate linear transformation. Specifically, it is shown that 8 × 8 S-boxes which possess good diffusion and nonlinearity properties may be effectively used as components of a secure block cipher. As well, it is demonstrated that the cipher may be strengthened by replacing the permutation of bits between S-box rounds with a diffusive linear transformation.

I. Introduction

Since its introduction in 1977, the Data Encryption Standard (DES) [1] has become the most widely applied private key block cipher. Recently, a hardware design to effectively break DES using exhaustive search was outlined by Wiener [2]. Unfortunately, since the DES design principles have never been fully disclosed, it is not generally known how to efficiently modify the DES algorithm to allow for different block or key sizes. This suggests that there is a need to replace DES with a secure, flexible block cipher whose design is well understood. In this paper, we contribute to the achievement of this objective by examining a simple, yet elegant class of block ciphers referred to as substitution-permutation networks or SPNs.

Feistel [3][4] was the first to suggest that an SPN architecture consisting of rounds of nonlinear substitutions (S-boxes) connected by bit position permutations was a simple, effective implementation of Shannon's concept of a "mixing transformation" based on the principles of "confusion" and "diffusion" [5]. Many modern block ciphers, including DES, FEAL [6], and LOKI [7], while deviating from Feistel's basic SPN model, are based on Shannon's fundamental concepts.

In this paper, we show that appropriately selected S-boxes and S-box interconnection transformations can be used to increase a cipher's resistance to differential [8] and linear cryptanalysis [9] and are also effective in improving a cipher's adherence to the important cryptographic property referred to as the strict avalanche criterion (SAC) [10]. In particular, we examine the use of large 8 × 8 S-boxes that are selected to provide strong diffusion and nonlinearity characteristics and we analyze the effectiveness of a novel application of linear transformations between rounds of S-boxes.

II. Background

We shall consider a general N-bit SPN as consisting of R rounds of $n \times n$ S-boxes. The plaintext and ciphertext are N-bit vectors denoted as

$\mathbf{P} = [P_1\ P_2\ ...\ P_N]$ and $\mathbf{C} = [C_1\ C_2\ ...\ C_N]$, respectively. An S-box in the network is defined as an n-bit bijective mapping S. A simple example of an SPN is illustrated in Figure 1.

In general, S-boxes may be keyed by (1) using key bits to select which mappings are used for the S-boxes or (2) XORing key bits with network bits prior to entering the S-boxes. We shall assume in our discussion that the network is keyed by XORing N bits of key (as determined by the key scheduling algorithm) before each round and after the last round of substitutions. Decryption is performed by running the data backwards through the network (i.e., applying the key scheduling algorithm in reverse and using the inverse S-boxes).

Rather than strictly confining ourselves to the basic form of S-boxes connected by a bit position permutation, in this paper we consider the more general model of S-boxes connected by invertible linear transformations. However, for consistency, we still refer to the more general architecture as an SPN.

III. Important Cryptographic Properties

In general, we consider that cryptographic properties may be categorized as either static or dynamic. Static properties encompass the relationships among plaintext, ciphertext, and key bits when the plaintext or key bits are not changing; dynamic properties refer to the relationships of plaintext, ciphertext, and key bit changes when a subset of plaintext or key bits are changed.

Important static properties include:

(S1) *completeness* [11]

- each ciphertext bit is a function of all plaintext and key bits

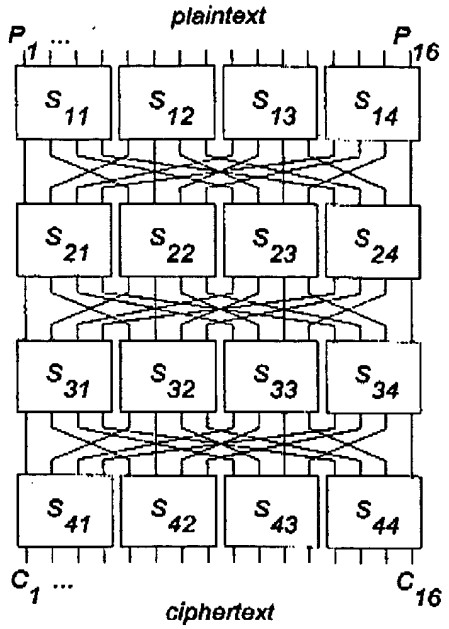

Figure 1. SPN with $N = 16$, $R = 4$, and $n = 4$

(S2) *nonlinearity* [12]

- each ciphertext bit has low correlation to a linear system equation

(S3) *static information theoretic properties* [13]

- partial knowledge of plaintext/key bits does not reveal any information about the ciphertext

Important dynamic properties include:

(D1) *strict avalanche criterion (SAC)* [10]

- a one bit plaintext/key change causes each ciphertext bit to change with a probability of 1/2

(D2) *low probability differential characteristics* [8]

- occurrence of a particular sequence of XOR differential pairs corresponding to each round is unlikely

(D3) *dynamic information theoretic properties* [13]

- partial knowledge of plaintext/key bit changes does not reveal any information about the ciphertext bit changes

The strict avalanche criterion and information theoretic properties — properties S3, D1, and D3 — can be considered as measures of a cipher's randomness and, hence, it's resistance to certain kinds of statistical attacks. For example, it can be shown that systems which do not satisfy SAC for key bit changes may be susceptible to key clustering attacks [14]. The remaining properties — S1, S2, D2 — are required to ensure immunity to clustering attacks [15], linear cryptanalysis [9], and differential cryptanalysis [8]. In this paper, we focus our attention on the properties of SAC, nonlinearity, and differential characteristics.

IV. S-box Design

In this section we discuss how S-boxes may be selected to provide the cryptographic properties of interest.

An important S-box property which is useful in improving resistance to differential cryptanalysis (by decreasing differential characteristic probabilities) is the rapid diffusion of bit changes [16][17][12]. (A simple example of S-box diffusion is the property that a one bit input change results in two or more output changes. We refer to this as first order diffusion and it is interesting to note that the DES S-boxes satisfy this property. Higher order diffusion is also possible [12].) As well, several authors [18][19][20] have suggested that selecting S-boxes with low probability XOR differential pairs is useful in ensuring low probability characteristics. In [17], O'Connor illustrates that for large n, the maximum XOR pair probability, p_δ, is expected to be small, $p_\delta \leq n/2^{n-1}$.

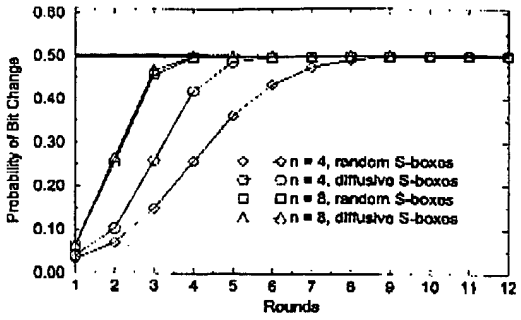

Figure 2. Experimental SAC for Different S-box Types

We propose selecting S-boxes to satisfy both diffusion and small XOR pair probabilities. In consideration of O'Connor's result, we have found that this is most easily done for large S-boxes. (Our experiments have involved S-boxes for which $n \leq 8$.) We have discovered that 8×8 S-boxes satisfying good diffusion characteristics may be efficiently selected using a depth-first-search algorithm. Among the S-boxes generated with good diffusion, it was easy to find S-boxes which were highly nonlinear ($NL \geq 96$) and satisfied $p_\delta \leq 2^{-4}$. Consider the following example.

Example 1: For an 8–round SPN, using 8×8 S-boxes which satisfy first order diffusion with $NL \geq 96$ and $p_\delta \leq 2^{-4}$, using reasonable assumptions about the permutations, it can be shown [12] that the minimum number of chosen plaintexts required for differential cryptanalysis is $N_D \approx 2^{40}$ and the number of known plaintexts required for linear cryptanalysis is $N_L \approx 2^{34}$. For a 64–bit block cipher using a 40–bit key, this SPN provides a reasonable level of security when compared to the 2^{40} key trials required in an exhaustive key search.

We consider that an SPN is stronger in relation to a criterion when fewer rounds are required to reasonably achieve the criterion. Using this definition of cryptographic strength, we have discovered that

(1) large S-boxes strengthen an SPN's SAC properties and

(2) strong diffusion characteristics strengthen an SPN's SAC properties (particularly for small S-boxes)

These conclusions are supported analytically in [21] and experimentally by the results presented in Figure 2. The curves of Figure 2 illustrate the probability of a ciphertext bit change as a function of the number of rounds in the network. The curves represent experimental data obtained for 64–bit SPNs using optimal permutations [21] and different sized S-boxes randomly selected to satisfy first order diffusion. The results presented are based on 10^4 randomly selected plaintexts and, if SAC was perfectly satisfied, we would expect the probability to be 1/2.

V. S-box Interconnection

In this section, we consider improving the security of an SPN by replacing the permutation between rounds of S-boxes with a suitable invertible linear transformation. Consider, for example, a linear transformation such as

$$\mathbf{V} = \pi(\mathcal{L}(\mathbf{U})) \tag{1}$$

where $\mathbf{V} = [V_1\ V_2\ ...\ V_N]$ is the vector of input bits to a round of S-boxes, $\mathbf{U} = [U_1\ U_2\ ...\ U_N]$ is the vector of bits from the previous round output, $\mathcal{L}(\mathbf{U}) = [L_1(\mathbf{U})\ ...\ L_N(\mathbf{U})]$ is a diffusive invertible linear transformation, and π is a permutation such that no two outputs of an S-box are connected to one S-box in the next round. The transformation $L_i(\mathbf{U})$ is given by

$$L_i(\mathbf{U}) = U_i \oplus Q \tag{2}$$

where $Q = U_1 \oplus U_2 \oplus ... \oplus U_N$.

Using such a transformation between rounds of S-boxes is useful in promoting rapid diffusion of bit changes. Let η_U represent the number of bit changes in vector $\mathbf{U}$ and η_V represent the number of bit changes in vector $\mathbf{V}$. It can be shown [21] that

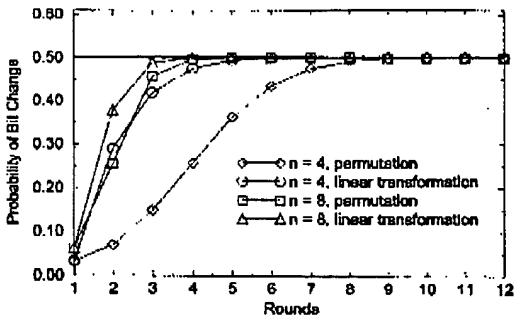

Figure 3. Experimental SAC for Linear Transformation

$$\eta_V = \begin{cases} \eta_U & ,\eta_U \text{ even} \\ N - \eta_U & ,\eta_U \text{ odd.} \end{cases} \tag{3}$$

Hence, a differential with a small, odd number of bit changes is translated into a differential with a large number of bit changes, whereas differentials with even changes remain unaffected. For example, if $N = 64$, a one bit change from the output of round r is translated into a 63 bit change to the input of round $r + 1$.

It can be shown [12] that the diffusion of bit changes by the linear transformation is useful in decreasing the upper bound on the differential characteristic probability when S-boxes are used which have no diffusion. As well, it may be demonstrated [12] that using such a linear transformation, the effectivenss of a linear approximation to the overall cipher can be decreased by requiring a larger number of S-box linear approximations to be included in the system linear expression.

Example 2: For an 8–round SPN, using 8×8 S-boxes which satisfy second order diffusion with $NL \geq 96$ and $p_\delta \leq 2^{-4}$ and using the linear transformation of (1), it can be shown [12] that $N_D \approx 2^{52}$ and $N_L \approx 2^{50}$. Note that, for a 64–bit SPN using a 64–bit key, the level of security is comparable to DES (with a 56–bit key) which has $N_D \approx 2^{47}$ and $N_L \approx 2^{47}$ and is reasonable when compared to the 2^{64} key trials required by exhaustive key search.

The diffusive effect of the linear transformation of (1) is also useful in strengthening the SAC properties of the SPN. Figure 3 illustrates the probability of a ciphertext bit change as a function of the number of network rounds based on 10^4 experimental plaintexts for a 64–bit SPN with different sized S-boxes.

VI. Key Scheduling

The keying mechanism is an important aspect of block cipher security. We recommend the application of a rotating key, that the sub-key applied at each round is unique, and that all key bits are applied as early as possible in the network.

It is interesting to note that the SPN structure considered in this paper is immune to the related-keys attack presented in [22]. In DES-like ciphers the related-keys attack exploits the half block of ciphertext that comes directly from the output of the previous round. In a basic SPN, it is not possible to examine the input to any round, thereby preventing any exploitation of the relationship between the sub-keys of consecutive rounds.

A block cipher is said to have a "weak" key if encryption using the key is equivalent to decryption using the same key. That is, double encryption of the plaintext results in the original plaintext. Since decryption does not use the same substitutions (the inverse S-boxes are used), the basic SPN structure has the advantage that there are no obvious weak keys. The keying structure itself has no apparent tendency to allow weak keys.

VII. Conclusions

In this paper, we have suggested that the basic SPN structure, motivated by Shannon and introduced by Feistel, is an elegant structure for the design of secure block ciphers. The case of randomly selecting large S-boxes that satisfy good diffusion and nonlinearity properties, combined with the simplicity of analyzing the network structure, support the use of such SPNs as the basis for secure block ciphers.

References

[1] National_Bureau_of_Standards, "Data Encryption Standard (DES)," *Federal Information Processing Standard Publication 46*, 1977.

[2] M. J. Wiener, "Efficient DES key search," *presented at CRYPTO '93*, Santa Barbara, Calif., Aug. 1993.

[3] H. Feistel, "Cryptography and computer privacy," *Scientific American*, vol. 228, no. 5, pp. 15–23, 1973.

[4] H. Feistel, W. A. Notz, and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications," *Proceedings of the IEEE*, vol. 63, no. 11, pp. 1545–1554, 1975.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[6] A. Shimizu and S. Miyaguchi, "Fast data encipherment algorithm: FEAL," *Advances in Cryptology: Proceedings of EUROCRYPT '87*, Springer-Verlag, Berlin, pp. 267–278, 1988.

[7] L. Brown, J. Pieprzyk, and J. Seberry, "LOKI - a cryptographic primitive for authentication and secrecy applications," *Advances in Cryptology: Proceedings of AUSCRYPT '90*, Springer-Verlag, Berlin, pp. 229–236, 1990.

[8] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[9] M. Matsui, "Linear cryptanalysis method for DES cipher," *Advances in Cryptology: Proceedings of EUROCRYPT '93*, Springer-Verlag, Berlin, pp. 386–397, 1994.

[10]A. F. Webster and S. E. Tavares, "On the design of S-boxes," *Advances in Cryptology: Proceedings of CRYPTO '85*, Springer-Verlag, Berlin, pp. 523–534, 1986.

[11]J. B. Kam and G. I. Davida, "A structured design of substitution-permutation encryption networks," *IEEE Transactions on Computers*, vol. 28, no. 10, pp. 747–753, 1979.

[12]H. M. Heys and S. E. Tavares, "Substitution-permutation networks resistant to differential and linear cryptanalysis," tech. rep., Department of Electrical Engineering, Queen's University, Oct. 22, 1993.

[13]M. Sivabalan, S. E. Tavares, and L. E. Peppard, "On the design of SP networks from an information theoretic point of view," *Advances in Cryptology: Proceedings of CRYPTO '92*, Springer-Verlag, Berlin, pp. 260–279, 1993.

[14]H. M. Heys and S. E. Tavares, "Key clustering in substitution-permutation network cryptosystems," *presented at Workshop on Selected Areas in Cryptography (SAC '94)*, Queen's University, Kingston, Canada, May 1994.

[15]D. Chaum and J. H. Evertse, "Cryptanalysis of DES with a reduced number of rounds," *Advances in Cryptology: Proceedings of CRYPTO '85*, Springer-Verlag, Berlin, pp. 192–211, 1986.

[16]L. R. Knudsen, "Iterative characteristics of DES and s^2-DES," *Advances in Cryptology: Proceedings of CRYPTO '92*, Springer-Verlag, Berlin, pp. 497–511, 1993.

[17]L. J. O'Connor, "On the distribution of characteristics in bijective mappings," *Advances in Cryptology: Proceedings of EUROCRYPT '93*, Springer-Verlag, Berlin, pp. 360–370, 1994.

[18]K. Nyberg, "Perfect nonlinear S-boxes," *Advances in Cryptology: Proceedings of EUROCRYPT '91*, Springer-Verlag, Berlin, pp. 378–386, 1991.

[19]M. H. Dawson and S. E. Tavares, "An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks," *Advances in Cryptology: Proceedings of EUROCRYPT '91*, Springer-Verlag, Berlin, pp. 352–367, 1991.

[20]C. M. Adams, "On immunity against Biham and Shamir's differential cryptanalysis," *Information Processing Letters*, vol. 41, no. 2, pp. 77–80, 1992.

[21]H. M. Heys and S. E. Tavares, "Avalanche characteristics of a class of product ciphers," tech. rep., Department of Electrical Engineering, Queen's University, Aug. 30, 1993.

[22]E. Biham, "New types of cryptanalytic attacks using related keys," *Advances in Cryptology: Proceedings of EUROCRYPT '93*, Springer-Verlag, Berlin, pp. 398–409, 1994.